

CH

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JAN 25 2008
JAN 25 2008
JUDGE AMY ST. EVE
United States District Court

C.H. ROBINSON WORLDWIDE, INC., a
Delaware Corporation,

Plaintiff,

v.

JEFFREY R. SIEKMANN, an individual,

Defendant.

Case No.

08C 0576

JUDGE AMY ST. EVE

MAGISTRATE JUDGE KEYS

**PLAINTIFF C.H. ROBINSON WORLDWIDE, INC.'S EMERGENCY MOTION FOR
TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTIVE RELIEF**

Plaintiff C.H. Robinson Worldwide, Inc. ("C.H. Robinson"), by its undersigned counsel, hereby moves this Honorable Court pursuant to Rule 65 of the Federal Rules of Civil Procedure for a Temporary Restraining Order and Preliminary Injunction against Defendant Jeffrey Siekmann ("Siekmann"). In support of this Motion, C.H. Robinson states as follows:

As set forth in the Verified Complaint and the other materials and evidence presented to the Court, including the Declaration of Jarrod Englebreton (annexed hereto as Exhibit A), this claim for injunctive relief arises from the conduct of Jeffrey Siekmann, an employee of C.H. Robinson, in obtaining highly confidential customer information from C.H. Robinson's secure database and emailing that information from his C.H. Robinson e-mail account to his personal e-mail account. On information and belief, Siekmann is currently seeking employment outside C.H. Robinson, suggesting that he intends to use C.H. Robinson's confidential business information to solicit C.H. Robinson's customers for another employer.

Through his conduct, Siekmann misappropriated C.H. Robinson's confidential and proprietary information and he now has disclosed and used, or threatens to disclose and use, that

information in breach of the confidentiality provisions of his employment related agreements with C.H. Robinson and in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*, and the Illinois Trade Secrets Act, 765 ILCS § 1065 *et seq.*

STATEMENT OF RELEVANT FACTS

A. C.H. Robinson and Its Business

C.H. Robinson is one of the industry leaders in the business of providing commercial logistics services, including the use of roads, highways, air, ocean and/or the railroad system, to transport or arrange for the transportation of goods in trailers and/or containers on behalf of third parties from a point of origin to their final destination throughout the United States and elsewhere (collectively "Freight Brokerage Services"). C.H. Robinson has contracts with thousands of independent carriers with whom it contracts to move freight on behalf of its customers.

In 1999, C.H. Robinson paid well over \$100 million to acquire substantially all of the assets of a logistics company called American Backhaulers ("Backhaulers"). While there were many facets to the transaction, one of the most integral components was the exclusive acquisition of a proprietary software program called Express. Express is a multi-faceted software program that allows C.H. Robinson to operate its business seamlessly across the world by, among other things, storing confidential information about its business and its customers; serving as the vehicle through which customer orders are placed; tracking order fulfillment; tracking customer and carrier status; identifying available loads, carriers and lanes for shipping; billing customers and tracking employee commissions. After acquiring Backhaulers, C.H. Robinson converted its entire business operation to the Express software system.

C.H. Robinson has invested millions of dollars to create a computerized network throughout the United States, proprietary software and acquire other software to insure that C.H.

Robinson can provide excellent logistics planning and service to its customers. Not only has C.H. Robinson invested in software to support its logistics planning and analysis, but it has also invested in software to permit its customers to electronically transmit and communicate their freight shipping needs to C.H. Robinson. Additionally, C.H. Robinson's computerized network allows its employees to communicate and share data through multiple servers, desktop computers and laptop computers throughout the United States as well as utilize the Internet for communication and selling efforts.

Prior to C.H. Robinson acquiring Backhaulers, in or about the mid-1990s, Backhaulers acquired DAV Transportation Services ("DAV"). Siekmann was employed by DAV at the time and became a Backhaulers employee. In December 1999, C.H. Robinson acquired all of the assets of Backhaulers including, but not limited to, Employee Non-Competition and Confidentiality Agreements, all rights to customized and proprietary software including Express, Backhaulers' know-how, and Backhaulers' intellectual property rights.

B. C.H. Robinson Secures Its Trade Secrets and Confidential Information

C.H. Robinson has invested substantial time and money gathering and developing confidential and proprietary information concerning its customers. This confidential and proprietary information includes, but is not limited to, customer contact information, sales information, credit information and detailed information about current customer requirements, preferences and purchase histories.

C.H. Robinson's proprietary information is not generally known in the industry and is valuable because C.H. Robinson derives economic value from the information not being publicly available. This proprietary business, software and customer information is of great value to C.H. Robinson and such information would give any competitor who improperly acquired such information an unfair competitive advantage. In addition, C.H. Robinson's customer

relationships and goodwill are of paramount importance to C.H. Robinson in that many of C.H. Robinson's customers have been customers for quite some time and hence, are long-term or near permanent customers. Moreover, in a number of instances, C.H. Robinson's customers entrust C.H. Robinson with confidential information.

Accordingly, C.H. Robinson protects its proprietary business and customer information by requiring employees to keep business, software and customer information confidential, by password protecting computers, by limiting access to information including access to Express, by requiring employees to sign data security agreements, by requiring employees to sign a certificate of compliance and by requiring employees to review its Code of Ethics. In addition, C.H. Robinson monitors employee e-mails, instant messages, and Internet usage. C.H. Robinson currently uses Symantec Compliance Accelerator software to monitor e-mails sent by employees. This software scans all sent e-mails and attachments for certain words and phrases. Members of C.H. Robinson's Employee Relations group then review those e-mails and attachments to determine if any policy violations have occurred. C.H. Robinson also uses Veritas Enterprise Vault software to capture and store all e-mails received and sent through the company's computer systems. E-mails captured by this software cannot be deleted by an employee.

C. Siekmann's Employment at C.H. Robinson

As an employee of C.H. Robinson, Siekmann has day-to-day contact with customers, vendors, and proprietary information and is entrusted with proprietary business and software information. This information includes, among other things: margin information, pricing, the identity of vendors, vendor pricing and relationship information, rate structures, marketing strategies, the identity of customers, customer transportation analysis information, software methodology information, customer contact information, container fleet information, detailed information about current customer requirements and preferences and purchase histories, source

code, object code, software functionality and other information which would give a competitor an unfair advantage in a competing business.

In exchange for his employment, monies, benefits and access to confidential information, Siekmann signed a Backhaulers' Employee Confidentiality and Non-Compete Agreement on or about March 25, 1998 in which he agreed that he would keep secret and confidential, and not use, disclose copy or assist any other person or firm in the use, disclosure or copying of C.H. Robinson's Confidential Information. Siekmann also agreed to return to C.H. Robinson all tangible records and documents relating to C.H. Robinson upon his termination or upon the request of C.H. Robinson.

In further exchange for his employment, monies, benefits and access to confidential information, Siekmann signed a C.H. Robinson Data Security Agreement on or about December 4, 1999 in which he agreed that any information such as customer lists, customer names, customer records, sales figures, and reports are confidential and shall not be retained or stored in any manner outside C.H. Robinson, including personal computers or elsewhere, and he signed a C.H. Robinson Internet and E-Mail Use Policy on or about December 4, 1999 in which he agreed that he would not use C.H. Robinson's e-mail/Internet for personal gain or in violation of C.H. Robinson's policies or applicable laws.

And in further exchange for his employment, monies, benefits and access to confidential information, Siekmann signed a C.H. Robinson Employee Agreement on or about February 28, 2005 and December 12, 2005 in which he agreed that he will never at any time use, disclose, copy or assist any other person or firm in the use, disclosure or copying of any C.H. Robinsons confidential information. Further, Siekmann agreed that he is prohibited for two years following employment termination from directly or indirectly soliciting, selling or rendering services to

any customer or prospective customer with which he worked or account for which he acquired confidential information during the two years prior to his termination from C.H. Robinson.

C.H. Robinson also requires its employees to complete compliance training and execute a hard copy or electronic certificate acknowledging compliance with C.H. Robinson's policies and Code of Ethics. Siekmann completed this program several times, including but not limited to, in 2006 and 2007.

D. Events Giving Rise to This Action

On January 15, 2008, C.H. Robinson Employee Relations personnel were reviewing e-mails from the Chicago Central office that had been captured by the Compliance Accelerator software. In doing so, it was discovered that 14 e-mails had been sent from Siekmann's C.H. Robinson e-mail account to an outside e-mail account identified as jsiek@cox.net. The content of the e-mails appeared suspicious because they were "screen shots" of entries in C.H. Robinson's Express database, where C.H. Robinson maintains confidential and proprietary customer and business information. The screen shots that Siekmann emailed outside the company contained highly confidential customer information including customer contacts, credit worthiness, recent business dealings, last quote date, D & B number, remaining credit and more.

The Veritas software was then employed on a few occasions to review all of Siekmann's e-mails sent from his C.H. Robinson account to the outside e-mail account for the period from January 1, 2008 to January 23, 2008. The review indicated that Siekmann had sent 127 e-mails from his C.H. Robinson account to his outside account during that time period, including the 14 e-mails discovered during the initial review using the Compliance Accelerator software. Over 125 e-mails contained screen shots of the Express database, five contained Express screen shots that included a list of customer information, three contained Excel spreadsheets, one contained a Microsoft Word document that included extremely detailed customer information and one

contained a PowerPoint client presentation. The review also revealed that the customers for which screen shots were taken by Siekmann were not customers that Siekmann services at C.H. Robinson. Rather, the customers are serviced by other C.H. Robinson employees.

Notably, the review revealed that Siekmann apparently attempted to hide his tracks by deleting from his "Outbox" the e-mails that he sent from his C.H. Robinson e-mail account to his personal e-mail account. In addition, it was discovered that Siekmann recently posted his resume to the careerbuilder.com website in an apparent attempt to obtain employment with a competitor to further benefit from the confidential information removed from C.H. Robinson.

C.H. Robinson never authorized Siekmann to e-mail or otherwise forward C.H. Robinson's confidential and proprietary information to an external e-mail account, it did not authorize Siekmann to view or remove data regarding customers that Siekmann did not service and it did not authorize Siekmann to destroy or delete e-mails. There was no legitimate reason for Siekmann to view confidential data regarding customers that he did not service. Thus, Siekmann is breaching his Agreements including without limitation his employment agreements, data security agreements, confidentiality agreements and code of ethics in at least one of the following ways by: (a) removing from, retaining or failing to return C.H. Robinson's confidential information; or (b) utilizing or disclosing confidential information of C.H. Robinson.

The proprietary business and customer information of C.H. Robinson constitute trade secrets because C.H. Robinson derives independent economic value from that information, such information is not generally known nor readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and because the information is the subject of reasonable efforts to maintain its secrecy. On information and belief, Siekmann will or has become employed by or affiliated with a competitor of C.H. Robinson and has unlawfully

and without authorization removed C.H. Robinson's trade secrets to benefit himself and/or a competitor and thus, will inevitably utilize or disclose C.H. Robinson's trade secrets and/or confidential information.

Siekmann removed from C.H. Robinson or retained its property without authorization, and converted it to his own use. C.H. Robinson has demanded from Siekmann the return of its property through its Code of Ethics, training and Agreements, but Siekmann has failed to return to C.H. Robinson its property.

C.H. Robinson's computer system is a protected computer and network which is used across state lines in interstate commerce, has Internet access across state lines and is used to transfer C.H. Robinson information for sales in interstate commerce. Siekmann was not authorized by C.H. Robinson to access its computer systems, access its computerized information, copy electronic information files, destroy electronic information files, send electronic information files to his personal e-mail account or continue to possess C.H. Robinson electronic files and data for personal gain or that of a competitor. C.H. Robinson faces irreparable injury and has suffered significant damages as a result of Siekmann's actions.

ARGUMENT

I. C.H. Robinson is Entitled to a TRO and a Preliminary Injunction Enjoining Siekmann from Violating the Terms of his Employment Related Agreements with C.H. Robinson and from Disclosing C.H. Robinson's Confidential and Proprietary Business Information.

A. The Standard for an Injunction.

An injunction is appropriate where a party demonstrates (1) some likelihood of succeeding on the merits, and (2) that it has "no adequate remedy at law" and will suffer "irreparable harm" if preliminary relief is denied. *Abbott Laboratories v. Mead Johnson & Co.*, 971 F.2d 6, 11 (7th Cir. 1992) (citation omitted). After satisfying this threshold inquiry, the

court must then consider: (3) the irreparable harm the non-moving party will suffer if preliminary relief is granted, balancing that harm against the irreparable harm to the moving party if relief is denied; and (4) the public interest, meaning the consequences of granting or denying the injunction to non-parties. *Id.* at 12.

In weighing these factors, the courts apply a “sliding scale” approach where “the stronger the case on the merits, the less irreparable the harm must be shown.” *Ty, Inc. v. GMA Accessories, Inc.*, 132 F.3d 1167, 1172 (7th Cir. 1997). In other words, if the harm to the plaintiff from denial of the preliminary injunction would be very great and the harm to the defendant from granting it very small, then the injunction should be granted even if the defendant has a better chance of prevailing on the merits than the plaintiff, provided the plaintiff’s chances are better than negligible. *Omega Satellite Prods. Co. v. City of Indianapolis*, 694 F.2d 119, 123 (7th Cir. 1982). Similarly, “[t]he more likely the plaintiff is to win, the less likely need the balance of harms weigh in his favor.” *Coca-Cola Co. v. Alma-Leo U.S.A., Inc.*, 719 F. Supp. 725, 727 (N.D. Ill. 1989) (quoting *Roland Machinery Co. v. Dresser Indus.*, 749 F.2d 380, 387 (7th Cir. 1984)).

B. C.H. Robinson Has a More Than Reasonable Likelihood of Success on the Merits.

To meet its burden of proof of likelihood of success, C.H. Robinson need only show that “it has a ‘better than negligible’ chance of succeeding on the merits.” *Meridian Mutual Ins. Co. v. Meridian Ins. Group, Inc.*, 128 F.3d 1111, 1114 (7th Cir. 1997). C.H. Robinson will likely succeed on all counts brought against Siekmann for violations of the Consumer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*, and the Illinois Trade Secrets Act, 765 ILCS § 1065 *et seq.* and for breach of contract.

1. C.H. Robinson Is Likely to Succeed on Its Claim for Violation of the Computer Fraud and Abuse Act.

A violation of the Computer Fraud and Abuse Act ("CFAA") occurs when, among other things, any person:

- (a) intentionally accesses a computer system without authorization or exceeds his authority to obtain information from a protected computer causing damage in excess of \$5,000.00 in violation of 18 U.S.C. § 1030(a)(2)(C); or
- (b) knowingly and with intent to defraud, accesses a protected computer without authorization or exceeds his authority, and by means of such conduct furthers the intended fraud and obtains valuable information resulting in damages exceeding \$5,000.00 in violation of 18 U.S.C. § 1030(a)(4); or
- (c) intentionally accesss a protected computer without authorization or exceeds his authority, and, as a result of such conduct, causes damage in excess of \$5,000.00 in violation of 18 U.S.C. § 1030(a)(5)(A)(iii).

The CFAA expressly provides plaintiffs (like C.H. Robinson) with a civil cause of action against those (like Siekmann) who would illegally use computers for their own commercial advantage. *See* 18 U.S.C. § 1030(g) ("any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief"). The Act defines "protected computer" broadly, as any high speed data process that "is used in interstate or foreign commerce or communication. *See* 18 U.S.C. § 1030(c)(2)(A)(B). Likewise, the Act broadly defines "damage" to include "any impairment to the integrity or availability of data, a program, a system or information "that causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals." *See* 18 U.S.C. § 1030(e)(8)(c).

C.H. Robinson's computer system is a protected computer network which is used across state lines in interstate commerce, has Internet access across state lines, and is used to transfer C.H. Robinson information for sales in interstate commerce. Siekmann was not authorized by C.H. Robinson to access its computer systems and computerized information for any purpose

other than to perform his duties as an employee of C.H. Robinson, nor was he authorized to copy electronic information files, destroy electronic information files, send electronic information files to his personal e-mail account or continue to possess C.H. Robinson electronic files and data for personal gain or that of a competitor. Thus, Siekmann plainly violated the statute by impermissibly accessing and forwarding confidential and proprietary customer information from C.H. Robinson's protected computer systems to his personal e-mail account, when this information was entirely unrelated to the scope of his employment with C.H. Robinson, when he apparently was seeking alternate employment, as evidenced by his posting of his resume on a job search website, and by destroying or deleting e-mails containing C.H. Robinson's confidential information.

Siekmann violated the Act when he accessed this protected information without authorization and for a purpose entirely unrelated to the scope of his employment, and then knowingly and with intent to misappropriate C.H. Robinson's confidential and proprietary business information, emailed that information to his personal e-mail account while acting for and on behalf of himself or perhaps others. *See Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006)(finding that defendant's breach of duty of loyalty to employer terminated his authority to access the employer's computer); *see also Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000) (enjoining former employees because they were no longer "authorized" to access employer's information once they began acting outside the scope of their employment). This is precisely what Siekmann did when he accessed and downloaded C.H. Robinson's proprietary information while also posting his resume to careerbulder.com. Therefore, C.H. Robinson will succeed on the merits of the Computer Fraud and Abuse Act claim.

2. C.H. Robinson Is Likely to Succeed on Its Claim for Violation of the Illinois Trade Secrets Act.

The Illinois Trade Secrets Act (“ITSA”) defines a “trade secret” as any type of information, including “technical or non-technical data,” “financial” information, and knowledge regarding “customers or suppliers,” which is (a) sufficiently secret to derive economic value... from not being generally known to other persons who can obtain economic value from its disclosure or sue; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality. 765 ILCS 1065/2(d). A person misappropriates a trade secret by, among other things, disclosing the trade secret despite knowing that it was “acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use.” 735 ILCS 1065/2(b)(2)(B)(II).

C.H. Robinson is entitled to injunctive relief for threatened and actual misappropriation by Siekmann. Specifically, the ITSA authorizes injunctive and other relief to remedy “actual or threatened misappropriation” of trade secrets. 765 ILCS 1065/3(a) (emphasis added). *See, e.g., Pepsico, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995) (holding that a plaintiff may prove a claim of trade secret misappropriation by demonstrating that defendant’s new employment will inevitably lead him to rely on the plaintiff’s trade secrets).

C.H. Robinson’s confidential business information—including customer contact information, requirements, preferences, and purchase histories—qualifies as “trade secrets” under the Act. C.H. Robinson’s confidential and proprietary information is not generally known in the industry and is valuable to C.H. Robinson because of its secrecy.

C.H. Robinson has spent millions of dollars developing and maintaining the information in its customer database. C.H. Robinson took reasonable measure to secure this confidential and proprietary information by, among other things, password-protecting its database and requiring

employees to comply with confidentiality policies. *See Multiut Corp. v. Draiman*, 359 Ill. App. 3d 527, 536, 834 N.E.2d 43, 50 (1st Dist. 2005) (affirming trial court's ruling that defendant took reasonable steps by limiting computer and hard-copy access to information and requiring confidentiality agreements); *Strata Marketing, Inc. v. Murphy*, 317 Ill. App. 3d 1054, 1069, 740 N.E.2d 1166, 1177 (1st Dist. 2000); *Gillis Assoc. Indus., Inc. v. Cari-All, Inc.*, 206 Ill. App. 3d 184, 564 N.E.2d 881 (1st Dist. 1990).

Siekmann violated the ITSA by impermissibly forwarding confidential and proprietary information from C.H. Robinson's computer systems when this information was of critical value to C.H. Robinson's business, C.H. Robinson had taken great measures to protect the information from disclosure, and Siekmann is and was well-aware of the need to maintain the confidentiality of this information. Moreover, the fact that he has posted his credentials on at least one job search website strongly suggests that he is seeking to change employers and will use C.H. Robinson's confidential customer information to solicit C.H. Robinson's customers on behalf of a new employer. This is actual and threatened misappropriation. C.H. Robinson respectfully submits that the ITSA was designed to prevent exactly this type of occurrence. Accordingly, C.H. Robinson is likely to succeed on the merits of this claim.

3. C.H. Robinson Is Likely to Succeed on Its Claim for Breach of Contract.

C.H. Robinson also will succeed on the merits of its claim for breach of contract because Siekmann violated his employment agreements, data security agreements, confidentiality agreements and code of ethics by removing from, retaining or failing to return C.H. Robinson's confidential information and/or by utilizing or disclosing confidential information belonging to C.H. Robinson.

C.H. Robinson is entitled to temporary and preliminary injunctive relief to enforce the restrictive covenants signed by Siekmann, including an Employee Confidentiality and Non-Compete Agreement, a Data Security Agreement, an Internet and E-Mail Use Policy, and an Employee Agreement that included confidentiality and non-solicitation provisions. Injunctive relief is appropriate because: (a) Siekmann's conduct threatens C.H. Robinson's legitimate, protectable interests in its confidential and proprietary information and in its long-term customer relationships; (b) the employment agreement is reasonably limited as to time and scope and (c) the non-solicitation provisions are limited to prospective or current customers of C.H. Robinson that Siekmann had contact with during the two years prior to termination. *See A-Tech Computer Servs., Inc. v. Soo Hoo*, 254 Ill. App. 3d 392, 399, 627 N.E.2d 21, 26 (1st Dist. 1993)("[a]n employer has a valid interest in protecting its long-standing client relationships against the subterfuge and sabotage of former employees").

Siekmann cannot be allowed to violate these provisions by utilizing C.H. Robinson's confidential and proprietary information for his personal benefit, offering C.H. Robinson's customers as an incentive for competitors to hire him, and soliciting C.H. Robinson's customers on behalf of another employer. Given these facts, C.H. Robinson is likely to succeed on its claim for breach of contract.

4. C.H. Robinson Is Likely to Succeed on Its Claim for Conversion

Finally, C.H. Robinson also will succeed on the merits of its claim for conversion because Siekmann removed from C.H. Robinson or retained its property without authorization, and converted it to his own use. C.H. Robinson demanded that Siekmann return its property through its Code of Ethics, training and Agreements, but Siekmann has failed to do so, resulting in considerable damage to C.H. Robinson in an amount to be determined at trial.

C. C.H. Robinson Will Likely Suffer Significant and Irreparable Harm If Injunctive Relief Is Not Granted.

Absent injunctive relief, C.H. Robinson will continue to be significantly and irreparably injured. Under Illinois law, a presumption of irreparable harm exists in cases of trade secret misappropriation. *Qsrsoft, Inc. v. Rest. Tech., Inc.*, No. 06 C 2734, 2006 U.S. Dist. LEXIS 76120, *33-34 (N.D. Ill. Oct. 19, 2006)(a copy is annexed as Exhibit B); *Computer Assocs. Int'l v. Quest Software, Inc.*, 333 F. Supp. 2d 688, 700 (N.D. Ill. 2004). A defendant can rebut this presumption only by establishing that the Plaintiff will not suffer any harm if the injunction is not granted. *Qsrsoft, Inc.*, 2006 U.S. Dist. LEXIS 76120 at *33; *Computer Assocs. Int'l*, 333 F. Supp. 2d at 700.

C.H. Robinson is threatened with losing customers, income and goodwill in amounts which may be impossible to determine unless Siekmann is enjoined and restrained by order of this Court. "Disclosure and use of the ex-employer's confidential information and trade secrets destroys the value of that information, permits the new employer to gain an unfair competitive advantage, and diminishes the ex-employer's competitive standing." *ISC-Bunker Ramo Corp. v. Altech, Inc.*, 765 F. Supp. 1310, 1335 (N.D. Ill. 1990)(court presumed irreparable injury from proof that a trade secret had been misappropriated).

If Siekmann's unlawful conduct is not restrained by this Court and is allowed to occur and continue, C.H. Robinson will suffer permanent and irreparable damages and injury through the disclosure of C.H. Robinson's confidential and proprietary information including, but not limited to, customer contact information and detailed information about current customer requirements, preferences, and purchase histories. Armed with C.H. Robinson's confidential information, Siekmann and any future employer of his will be able to solicit C.H. Robinson's customers and gain an unfair competitive edge in the industry, thus irreparably damaging C.H.

Robinson's business relationships and its future business. Siekmann and his future employer will be spared immeasurable expense, time and burden in accumulation of client information and development of customer goodwill.

C.H. Robinson will never be able to know how many market opportunities it missed, how many sales it did not make, or how many customers it lost if Siekmann is free to misappropriate C.H. Robinson's confidential information. There is thus no way that a money judgment after trial on the merits can completely compensate C.H. Robinson for Siekmann's misappropriations, and only injunctive relief will adequately address the substantial risk of irreparable harm that C.H. Robinson faces.

D. The Balance of Hardships and Public Interest Weight Heavily in Favor of Granting C.H. Robinson's Request for Injunctive Relief.

If Siekmann's conduct is permitted to occur and continue, C.H. Robinson will suffer more from the denial of an injunction than Siekmann would suffer from the issuance of an injunction, and greater injury will be inflicted upon C.H. Robinson by the denial of relief than would be inflicted upon Siekmann by the granting of relief. An injunction would force the return of C.H. Robinson's property, prohibit Siekmann from further disclosing or utilizing C.H. Robinson's confidential business information, and protect C.H. Robinson's goodwill and customer relationships. On the other hand, no injury will be inflicted upon Siekmann by issuance of injunctive relief because such relief will require Siekmann to refrain from plainly prohibited conduct and will prevent him from benefiting from his own misconduct. *See Merrill Lynch v. Cross*, No. 99 C 1435, 1998 U.S. Dist. LEXIS 3188, * 6 (N.D. Ill. Mar. 12, 1998) (holding that harm to plaintiff from disclosure of its clients' financial information outweighed harm to defendant from refraining from using plaintiff's trade secrets and customer information for a short period of time)(a copy is annexed as Exhibit C); *ISC-Bunker Ramo Corp.*, 765 F.

Supp. at 1335 (holding that balance of hardships weighs in favor of plaintiff who stands to lose value of its trade secrets if defendant is not enjoined from using plaintiff's misappropriated computer programs and manuals).

E. C.H. Robinson Has No Adequate Remedy At Law.

Under Illinois law, a remedy at law is *per se* inadequate if it is not "concise, complete and [does not] provide the same practical and efficient resolution as the equitable remedy would provide." *Hough v. Weber*, 202 Ill. App. 3d 674, 687, 560 N.E.2d 5, 15 (2d Dist. 1990) (internal citations omitted). Equitable remedies are also necessary to enforce contractual provisions or benefits which a plaintiff "did not receive" due to defendant's breach of that agreement. *See, e.g., Prairie Eye Ctr., Ltd. v. Butler*, 329 Ill. App. 3d 293, 304, 768 N.E.2d 414, 424 (4th Dist. 2002), *appeal denied*, 202 Ill. 2d 661, 787 N.E.2d 169 (2002) (affirming permanent injunction as remedy for breach of contract). By definition, a remedy at law is a backwards-looking remedy and thus inadequate compared to injunctive relief which, for example, can halt ongoing breaches of contract or preclude them entirely. *See, e.g., Willett Motor Coach Co. v. Bd. of Educ. of City of Chicago*, 171 Ill. App. 3d 166, 170, 524 N.E.2d 1155, 1158 (1st Dist. 1988) (enjoining breach of contract and directing compliance with contractual terms).

This is an entirely appropriate case for injunctive relief, because it is impossible to fully compensate C.H. Robinson for its loss if Siekmann is allowed to disclose and use C.H. Robinson's confidential customer information to solicit those customers. *See ISC-Bunker Ramo Corp.*, 765 F. Supp. at 1335 ("Disclosure and use of the ex-employer's confidential information and trade secrets destroys the value of that information, permits the new employer to gain an unfair competitive advantage, and diminishes the ex-employer's competitive standing.").

Thus, consistent with Illinois law, an injunction here is the only way to preserve the benefit of C.H. Robinson's bargain regarding the confidentiality and non-solicitations covenants

it obtained from Siekmann. Moreover, as discussed above, the Illinois Trade Secrets Act provides an equitable remedy to prevent the misappropriation of trade secrets, whether that misappropriation has occurred or is threatened to occur. 765 ILCS 1065/3(a). For these reasons, C.H. Robinson demonstrates a lack of an adequate remedy at law.

CONCLUSION

For the reasons stated above, C.H. Robinson has shown a likelihood of success on the merits of its claims, that it will suffer irreparable harm, that it is without an adequate remedy at law, that the balance of equities weighs in its favor, and that an injunction would serve the public interest. WHEREFORE, C.H. Robinson respectfully prays that this Court enter an order that:

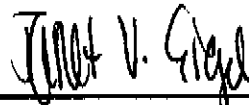
- (a) orders Siekmann to account for the whereabouts of and to return all of C.H. Robinson's confidential and/or proprietary information,
- (b) enjoins Siekmann from disclosing or using C.H. Robinson's confidential and/or proprietary information,
- (c) orders Siekmann to produce for inspection all computers in his possession, custody and/or control on which C.H. Robinson information may reside,
- (d) orders Siekmann to provide access for inspection to the outside e-mail account jsiek@cox.net to which he emailed C.H. Robinson information from his C.H. Robinson e-mail account and any other e-mail account for which he has custody or control,
- (e) enjoins Siekmann from contacting or conducting business with any C.H. Robinson customer whose information he improperly accessed and/or misappropriated,
- (f) enjoins Siekmann from contacting or conducting business with any C.H. Robinson customer with whom he conducted business on behalf of C.H. Robinson within the twenty-four (24) months preceding this Court's Order, and
- (g) grants such other and further relief as this Court deems just and proper.

No prior application for the relief requested herein has been made to this or any other Court. A draft Order is attached hereto as Exhibit D.

DATED: January 25, 2008

Respectfully submitted,

C.H. ROBINSON WORLDWIDE, INC.

By 
One of Its Attorneys

Michael D. Wexler
Janet V. Siegel
SEYFARTH SHAW LLP
131 South Dearborn Street, Suite 2400
Chicago, Illinois 60603
(312) 460-5000

A

DECLARATION OF JARROD ENGLEBRETSON

Pursuant to 28 U.S.C. § 1746, I, Jarrod Englebreton, state that if called as a witness in this case, I could competently and truthfully testify on personal knowledge as to the following facts:

1. I am over the age of 18 and am under no physical or mental disability that limits my ability to testify truthfully to the matters stated in this declaration.

2. I have been employed by C.H. Robinson Worldwide ("C.H. Robinson") for five years. For the past four years I have managed the Employee Relations group and for the past two years held the title of Director of Employee Relations.

3. As Director of Employee Relations, I am responsible for managing a team of people who work with managers and executives throughout the company on issues and projects related to compliance and employee engagement. Among other areas within my job responsibilities is ensuring compliance with C.H. Robinson's Electronic and Data Communications Policy.

4. I submit this declaration in support of C.H. Robinson's Motion for a Temporary Restraining Order and for a Preliminary Injunction.

C.H. ROBINSON AND ITS BUSINESS

5. C.H. Robinson is a Delaware corporation with its corporate headquarters and principal place of business located in Eden Prairie, Minnesota. C.H. Robinson is a national leader in the business of providing commercial third party logistics services for the transportation of freight throughout the United States and elsewhere. C.H. Robinson has employees throughout the country.

C.H. ROBINSON'S CONFIDENTIAL AND PROPRIETY INFORMATION

6. C.H. Robinson has invested substantial time and money gathering and developing confidential and proprietary information concerning our customers. This confidential and proprietary information includes, but is not limited to, customer contact information and detailed information about current customer requirements, preferences, and purchase histories.

C.H. ROBINSON PROTECTS ITS INFORMATION

7. C.H. Robinson requires that its confidential and proprietary information be kept strictly confidential by its employees and restricts access to this information. C.H. Robinson uses secure, password-protected databases to organize, maintain, secure, and access its confidential and propriety information.

8. Among the many measures that C.H. Robinson implements to protect its information is the Electronic and Data Communications Policy. In support of this policy, C.H. Robinson monitors employee e-mails, instant messages, and Internet usage. C.H. Robinson currently uses Symantec Compliance Accelerator software to monitor e-mails sent by employees. This software scans all sent e-mails and attachments for certain words and phrases. Members of C.H. Robinson's Employee Relations group then review those e-mails and attachments to determine if any policy violations have occurred. C.H. Robinson also uses Veritas Enterprise Vault software to capture and store all e-mails received and sent through the company's computer systems. Emails captured by this software cannot be deleted by an employee.

DISCOVERY OF JEFFREY SIEKMANN'S MISAPPROPRIATION OF C.H. ROBINSON'S CONFIDENTIAL AND PROPRIETY BUSINESS INFORMATION

9. Jeffrey Siekmann has been employed by C.H. Robinson since the mid-1990's. Siekmann is a customer account representative. He is an employee of C.H. Robinson's Chicago Central branch office located in Chicago, Illinois, however he works from his home in Arizona.

Siekmann reports to supervisors who are located in the Chicago office and he travels to Chicago several times per year for business related meetings or conferences.

10. On January 15, 2008, I was reviewing e-mails from the Chicago branch office that had been captured by the Compliance Accelerator software. In doing so, I discovered 14 e-mails that had been sent from Siekmann's C.H. Robinson email account to an outside email account identified as jsiek@cox.net. The content of the e-mails appeared suspicious to me because they were "screen shots" of entries in C.H. Robinson's Express database, where C.H. Robinson maintains confidential and proprietary customer and business information. The screen shots that Siekmann had emailed outside the company contained highly confidential customer information including customer contacts, credit worthiness, recent business dealings, last quote date, D & B number, remaining credit and more.

11. Upon viewing these e-mails, I notified Pat Nolan, a Director, in the Chicago Central branch office and informed him that I would further investigate by using the Veritas software to review all of Siekmann's e-mails sent from his C.H. Robinson account to the outside email account for the period from January 1, 2008 to January 15, 2008. My review of those e-mails and subsequent reviews through January 23, 2008, indicated that Siekmann had sent 127 e-mails from his C.H. Robinson account to his outside account during that time period, including the 14 e-mails discovered during my initial review using the Compliance Accelerator software. Of the e-mails, over 125 contained screen shots of the Express database, five contained Express screen shots that included a list of customer information, three contained Excel spreadsheets, one contained a Microsoft Word document that included extremely detailed customer information and one contained a PowerPoint client presentation.. My review also revealed that the customers

for which screen shots were taken by Siekmann were not customers that Siekmann services at C.H. Robinson. Instead, the customers are serviced by other C.H. Robinson employees.

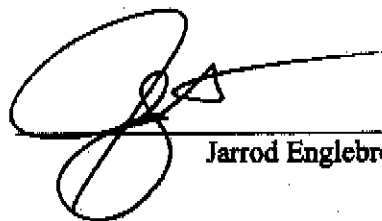
12. It was also discovered that Siekmann apparently attempted to hide his tracks by deleting the e-mails that he sent from his C.H. Robinson e-mail account from his "Outbox".

13. C.H. Robinson never authorized Siekmann to email or otherwise forward C.H. Robinson's confidential and proprietary information to an external email account, it did not authorize Siekmann to view or remove data regarding customers that Siekmann did not service and it did not authorize Siekmann to delete or destroy electronic e-mails or files from his C.H. Robinson e-mail account. Moreover, there would be no legitimate business reason for Siekmann to view and copy confidential data regarding customers that he did not service.

14. It was also discovered that Siekmann recently posted his resume to the careerbuilder.com website in an apparent attempt to obtain employment with a competitor to further benefit from the confidential information removed from C.H. Robinson.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on January 25th, 2008.

A handwritten signature in black ink, appearing to read 'Jarrod Englebretson', is written over a horizontal line.

Jarrod Englebretson

B

LEXSEE 2006 U.S. DIST. LEXIS 76120



Analysis

As of: Jan 25, 2008

QSRSoft, INC. Plaintiff, v. RESTAURANT TECHNOLOGY, INC., et al., Defendants.

No. 06 C 2734

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

2006 U.S. Dist. LEXIS 76120; 84 U.S.P.Q.2D (BNA) 1297

October 19, 2006, Decided

SUBSEQUENT HISTORY: Motion granted by, in part, Motion denied by, in part, Claim dismissed by *QSRSoft, Inc. v. Rest. Tech.*, 2006 U.S. Dist. LEXIS 80729 (N.D. Ill., Nov. 2, 2006)

CASE SUMMARY:

PROCEDURAL POSTURE: Plaintiff, provider of software for assisting franchisees to analyze information collected from restaurants, alleged that defendant, another software provider, violated the Copyright Act of 1976, 17 U.S.C.S. 101 et seq., and the Illinois Trade Secret Act (ITSA), 765 Ill Comp. Stat. 1065/1 et seq., by accessing and copying its software to develop a similar product. Plaintiff moved for entry of a preliminary injunction against defendant.

OVERVIEW: The plaintiff software provider alleged that defendant used a password provided with restrictions in order to gain access to the plaintiff's software and use to it to develop its own similar software. The court found that there was sufficient evidence showing that plaintiff met its burden to show a prima facie presumption of validity with respect to its copyright. Therefore, plaintiff had a strong likelihood of showing that defendant copied original elements of its copyrighted website. The court also found that the evidence showed that plaintiff was likely to succeed in establishing the existence of valid trade secrets, given that plaintiff's secrets were sufficiently guarded from the public. Plaintiff's efforts to guard its system with licensing agreements and a password protected website were more than reasonable to

establish a better than negligible chance that plaintiff would be able to show that it did not waive its trade secrets. Thus, the court concluded that there was a strong likelihood that plaintiff's claimed trade secrets were protected by the ITSA and that defendant misappropriated its trade secrets.

OUTCOME: The court granted plaintiff's motion for a preliminary injunction.

LexisNexis(R) Headnotes**Civil Procedure > Remedies > Injunctions > Preliminary & Temporary Injunctions**

[HN1] A preliminary injunction should not be granted unless the movant, by a clear showing, carries the burden of persuasion. When determining whether to use such a remedy, the district court has to arrive at a decision based on a subjective evaluation of the import of the various factors and a personal, intuitive sense about the nature of the case.

Civil Procedure > Remedies > Injunctions > Preliminary & Temporary Injunctions

[HN2] In order to obtain a preliminary injunction, a plaintiff must show that: (1) the plaintiff has a reasonable likelihood of success on the merits; (2) no adequate remedy at law exists; (3) the plaintiff will suffer irreparable harm which, absent injunctive relief, outweighs the irreparable harm the respondent will suffer if the injunc-

2006 U.S. Dist. LEXIS 76120, *; 84 U.S.P.Q.2D (BNA) 1297

tion is granted; and (4) the injunction will not harm the public interest. A likelihood of success means that the party has a better than negligible chance of succeeding on the merits. Once the above four conditions are satisfied, the court evaluates the likelihood of success on a sliding scale. The factors in the sliding scale analysis include the irreparable harm the party would endure without the preliminary injunction, any irreparable harm the opposing party will suffer as a result of the preliminary injunction, and any harm or benefit to the public if the injunction is granted or denied. The sliding scale works in such a way that a lesser likelihood of success may support a preliminary injunction if the balance of harms favors the party seeking the remedy. Likewise, a stronger likelihood of success permits granting a preliminary injunction even if the balance of harms is not necessarily in the seeking party's favor.

Civil Procedure > Remedies > Injunctions > Preliminary & Temporary Injunctions

Copyright Law > Civil Infringement Actions > Elements > General Overview

Copyright Law > Civil Infringement Actions > Remedies > Injunctive Relief

[HN3] 17 U.S.C.S. § 502(a) of the Copyright Act authorizes courts to issue a preliminary injunction on such terms as the court may deem reasonable to prevent or restrain infringement of a copyright. 17 U.S.C.S. § 502(a). Irreparable injury may be presumed upon the showing of a prima facie case of copyright infringement. To prevail on a copyright infringement claim, a plaintiff must prove that (1) the plaintiff owned a valid copyright, and (2) defendant copied original elements, or infringement, of the work.

Copyright Law > Civil Infringement Actions > Presumptions & Requirements > Presumption of Copyright Validity

[HN4] See 17 U.S.C.S. § 410(c).

Copyright Law > Civil Infringement Actions > Presumptions & Requirements > Presumption of Copyright Validity

[HN5] The presumption of validity and ownership of a copyright is rebuttable.

Copyright Law > Civil Infringement Actions > Elements > General Overview

[HN6] Facts, whether alone or as part of a compilation, are not original and therefore may not be copyrighted. A factual compilation is eligible for copyright if it features

an original selection or arrangement of facts, but the copyright is limited to the particular selection or arrangement. In no event may copyright extend to the facts themselves.

Copyright Law > Civil Infringement Actions > Elements > General Overview

[HN7] The Copyright Act defines direct infringement as anyone who violates any of the exclusive rights of the copyright owner. 17 U.S.C.S. 501(a).

Copyright Law > Civil Infringement Actions > Infringement Online > General Overview

[HN8] Uploading files containing copyrighted photographs constitute reproduction.

Copyright Law > Civil Infringement Actions > Elements > Substantial Similarity > General Overview

[HN9] For purposes of copyright infringement claims, the law of the United States Court of Appeals for the Seventh Circuit does not require a side-by-side comparison of products, but rather requires a substantial similarity between the plaintiff's copyrighted work and the defendant's work if there is no evidence of direct infringement.

Copyright Law > Civil Infringement Actions > Remedies > Injunctive Relief

[HN10] Under the Illinois Trade Secret Act (ITSA), 765 Ill. Comp. Stat. 1065/1 et seq., the court may issue an injunction if there is actual or threatened misappropriation of a trade secret. 765 Ill. Comp. Stat. 1065/3(a).

Trade Secrets Law > Misappropriation Actions > Elements > General Overview

[HN11] For a plaintiff to show a better than negligible chance on succeeding on its trade secret misappropriation claim under the Illinois Trade Secret Act (ITSA), 765 Ill. Comp. Stat. 1065/1 et seq., it must show that (1) there is a trade secret; (2) the trade secret was misappropriated by defendant; and (3) defendant used the trade secret for business purposes.

Trade Secrets Law > Misappropriation Actions > Elements > General Overview

[HN12] The Illinois Trade Secret Act (ITSA), 765 Ill. Comp. Stat. 1065/1 et seq., defines a trade secret as: Information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program,

2006 U.S. Dist. LEXIS 76120, *; 84 U.S.P.Q.2D (BNA) 1297

device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that: (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality. 765 Ill. Comp. Stat. 1065/2(d). The ITSA therefore precludes trade secret protection for information generally known or understood within an industry even if not to the public at large, and requires a plaintiff to take affirmative measures to prevent others from using the information.

Trade Secrets Law > Factors > General Overview

[HN13] In determining whether a trade secret exists, Illinois courts generally look to: (1) the extent that the information is known outside of the business; (2) the extent that the information is known to employees and others within the business; (3) the measures taken to protect the information from outsiders; (4) the value of the information to competitors; (5) the amount of time, money, and effort to develop the information; and (6) the ease that the information could be acquired by others.

Trade Secrets Law > Protection of Secrecy > General Overview

[HN14] Trade secret is not waived when reasonable efforts are taken to protect secrecy of trade secrets from competitors.

Trade Secrets Law > Misappropriation Actions > General Overview

[HN15] See 765 Ill. Comp. Stat. 1065/2(b).

Trade Secrets Law > Misappropriation Actions > Elements > Improper Means

[HN16] The Illinois Trade Secret Act (ITSA), 765 Ill. Comp. Stat. 1065/1 et seq., defines "improper means" to include theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means. 765 Ill. Comp. Stat. 1065/2(a).

Trade Secrets Law > Breach of Contract > Implied Contracts

[HN17] An implied-in-fact contract is one in which an agreement may be inferred by performance of the parties.

Copyright Law > Civil Infringement Actions > Remedies > Injunctive Relief

[HN18] There is a rebuttable presumption of irreparable harm to a plaintiff in cases of trade secret misappropriation and copyright infringement. A defendant can rebut this presumption by demonstrating that the plaintiff will not suffer any harm if the injunction is not granted.

Copyright Law > Civil Infringement Actions > Remedies > Damages > General Overview

[HN19] It is virtually impossible to ascertain the precise economic consequences of intangible harms, such as damage to reputation and loss of goodwill.

Copyright Law > General Overview

[HN20] The public is generally interested in upholding intellectual property rights, encouraging innovation and creativity, and rewarding those that take the risk and invest resources in pursuit of such innovation and creativity.

COUNSEL: [*1] For Qsrsoft, Inc., an Illinois Corporation, Plaintiff: Jonathan Mandel Weis, Josh Slater Kaplan, Mitchell S. Chaban, Levin Ginsburg, Chicago, IL.

For Restaurant Technology, Inc., a Georgia Corporation, Defendant: Darren Steven Cahr, David J Moorhead, Gardner Carton & Douglas LLP, Chicago, IL; Jeanine Gibbs, Joseph D. Wargo, Julie C. Jared, Michael S French, Wargo & French LLP, Atlanta, GA.

For James H. Clutter, an individual, J Neal Starkey, an individual, Defendants: Darren Steven Cahr, David J Moorhead, Gardner Carton & Douglas LLP, Chicago, IL; Jeanine Gibbs, Julie C. Jared, Michael S French, Wargo & French LLP, Atlanta, GA.

JUDGES: Samuel Der-Yeghiayan, United States District Court Judge.

OPINION BY: Samuel Der-Yeghiayan

OPINION

MEMORANDUM OPINION

SAMUEL DER-YEGHIAYAN, District Judge

This matter is before the court on Plaintiff QSRSoft, Inc.'s ("QSRSoft") motion for entry of a preliminary injunction against Defendant Restaurant Technology, Inc. ("RTI"). For the reasons stated below, we grant QSRSoft's motion for a preliminary injunction.

2006 U.S. Dist. LEXIS 76120, *; 84 U.S.P.Q.2D (BNA) 1297

BACKGROUND

QSRSoft contends that every McDonald's Restaurant has a McDonald's Corporation computer system, an in store processor [*2] ("ISP"), that stores data about the restaurant's sales performance and status. McDonald's Corporation allegedly provides restaurant operators with limited reports, called R2D2, but in no relation to Star Wars, generated from the ISP data. Additionally, QSRSoft alleges that McDonald's Corporation has approved QSRSoft and RTI as back-office vendors, meaning that each has access to the data stored in the ISP. Both QSRSoft and RTI provide software tools to McDonald's Restaurant franchise owners and operators ("franchisees"). QSRSoft contends that both companies' software tools use data extracted from the ISP.

QSRSoft alleges that it developed the DotComm System, an internet-based computer system that assists franchisees in analyzing information collected from the restaurants. QSRSoft contends that the DotComm System differs from other competitors' systems in that it more quickly collects and processes information from restaurants, provides automatic information transfer backup, and provides underlying detail or reports. QSRSoft alleges that if a franchise wants to use the DotComm System, the franchisee must first obtain a licensing agreement, which includes a provision that only key management [*3] personnel are permitted to access the DotComm System due to its proprietary nature. According to QSRSoft, a franchisee is provided with the opportunity to evaluate the DotComm System for thirty days under the terms of a software evaluation licensing agreement. QSRSoft contends that once the franchisee agrees to the licensing agreement and identifies a list of the key personnel that will have access to the DotComm System, QSRSoft sends the franchisee an access code and unique password. QSRSoft alleges that the DotComm System automatically instructs the user to change the password during the first time the franchisee accesses the system. According to QSRSoft, the franchisee informs QSRSoft of the updated password.

QSRSoft claims that in January 2006, RTI, who provides predominantly accounting software to fast food restaurants, contacted F.A.F., Inc. d/b/a McDonald's Restaurant ("FAF"), which operates nine McDonald's restaurants in Fargo, North Dakota, to obtain information from QSRSoft about the DotComm System. QSRSoft contends that in February 2006, Gregg Matejka ("Matejka"), FAF's director of operations, contacted QSRSoft about evaluating the DotComm System in one of FAF's McDonald's [*4] restaurants. QSRSoft claims that it subsequently sent a licensing agreement ("Agreement") to FAF and requested that the Agreement be executed and returned to QSRSoft. QSRSoft further alleges that on

February 8, 2006, QSRSoft sent an access code and password to FAF in anticipation of receiving the executed Agreement from FAF. Although FAF did not return the Agreement, QSRSoft contends that FAF understood that FAF was accepting the terms of the Agreement and would use the DotComm System subject to such terms. QSRSoft claims that on February 8, 2006, FAF accessed the DotComm System using the newly provided access code and password, a process that required FAF to change the initial password. According to QSRSoft, on or about February 9, 2006, FAF provided RTI with the access code and the recently changed password ("FAF password").

QSRSoft alleges that RTI used the FAF password from February 2006 until April 30, 2006 in order to gain access to the DotComm System, view, download, save, print, and copy each web page on the DotComm System, as well as to download the QSRSoft Data Engine, the backbone of the DotComm System's ability to extract restaurant information. QSRSoft claims that RTI [*5] was able to use the information it received from accessing the DotComm System to develop Reports+, a similar RTI product for McDonald's franchises.

On August 8, 2006, QSRSoft filed an amended complaint that includes claims alleging copyright infringement under the Copyright Act of 1976, 17 U.S.C. 101 *et seq.* ("Copyright Act") brought against RTI (Count I), James H. Clutter ("Clutter") (Count II), and J. Neal Starkey ("Starkey") (Count III), claims alleging violations of the Illinois Trade Secret Act, 765 ILCS 1065/1 *et seq.*, ("ITSA") brought against RTI, Clutter, and Starkey (Count IV), conversion claims brought against RTI, Clutter, and Starkey (Count V), tortious interference with prospective business advantage claims brought against RTI, Clutter, and Starkey (Count VI), and tortious interference with contract claims brought against RTI, Clutter, and Starkey (Count VII).

On August 23, 2006, RTI filed a partial motion to dismiss Counts IV, V, and VII. On October 18, 2006 we denied RTI's partial motion to dismiss to the extent that it related to Counts IV and VII, and granted the motion to dismiss to the extent that it related [*6] to Count V. QSRSoft now seeks a preliminary injunction.

LEGAL STANDARD

[HN1] A preliminary injunction "should not be granted unless the movant, by a clear showing, carries the burden of persuasion." *Goodman v. Ill. Dept. of Fin. & Prof'l Regulation*, 430 F.3d 432, 437 (7th Cir. 2005)(stating that "[a]s the Supreme Court has observed, '[a] preliminary injunction is an extraordinary and drastic remedy'"(quoting *Mazurek v. Armstrong*, 520 U.S. 968, 972, 117 S. Ct. 1865, 138 L. Ed. 2d 162 (1997))). When

determining whether to use such a remedy, "the district [court] has to arrive at a decision based on a subjective evaluation of the import of the various factors and a personal, intuitive sense about the nature of the case." *Faheem-El v. Klincar*, 841 F.2d 712, 717 (7th Cir. 1988)(quoting *Lawson Products, Inc. v. Avnet, Inc.*, 782 F.2d 1429, 1436 (7th Cir. 1986)).

[HN2] In order to obtain a preliminary injunction, a plaintiff must show that: "(1) [the plaintiff] ha[s] a reasonable likelihood of success on the merits; (2) no adequate remedy at law exists; (3) [the plaintiff] will suffer irreparable harm which, absent injunctive relief, outweighs the [*7] irreparable harm the respondent will suffer if the injunction is granted; and (4) the injunction will not harm the public interest." *Goodman*, 430 F.3d at 437. A likelihood of success means that the party has a "better than negligible chance" of succeeding on the merits. *Washington v. Ind. High Sch. Ath. Ass'n*, 181 F.3d 840, 845 (7th Cir. 1999). Once the above four conditions are satisfied, the court evaluates the likelihood of success on a sliding scale. *AM General Corp. v. DaimlerChrysler Corp.*, 311 F.3d 796, 804 (7th Cir. 2002). The factors in the sliding scale analysis include the irreparable harm the party would endure without the preliminary injunction, any irreparable harm the opposing party will suffer as a result of the preliminary injunction, and any harm or benefit to the public if the injunction is granted or denied. *AM General Corp.*, 311 F.3d at 803-04; *Ty, Inc. v. Jones Group, Inc.*, 237 F.3d 891, 895 (7th Cir. 2001). The sliding scale works in such a way that a lesser likelihood of success may support a preliminary injunction if the balance of harms favors the party seeking the remedy. [*8] *Ty*, 237 F.3d at 895; *Eli Lilly & Co. v. Natural Answers, Inc.*, 233 F.3d 456, 461 (7th Cir. 2000). Likewise, a stronger likelihood of success permits granting a preliminary injunction even if the balance of harms is not necessarily in the seeking party's favor. *Bloedorn v. Francisco Foods, Inc.*, 276 F.3d 270, 298 (7th Cir. 2001).

DISCUSSION

I. Reasonable Likelihood of Success on the Merits

A. Copyright Claims

[HN3] Section 502(a) of the Copyright Act authorizes the court to issue a preliminary injunction "on such terms as [the court] may deem reasonable to prevent or restrain infringement of a copyright." 17 U.S.C. § 502(a). Irreparable injury may be presumed upon the showing of a *prima facie* case of copyright infringement. *Atari Inc. v. North Am. Philips Consumer Elec. Corp.*, 672 F.2d 607, 620 (7th Cir. 1982). To prevail on a copyright infringement claim, QSRSoft must prove that (1) QSRSoft

owned a valid copyright, and (2) RTI copied original elements, or infringement, of the work. *Feist Publ'ns, Inc. v. Rural Telephone Serv. Co., Inc.*, 499 U.S. 340, 361, 111 S. Ct. 1282, 113 L. Ed. 2d 358 (1991). [*9]

1. Copyright Validity

QSRSoft has registered copyrights in the Data Engine, Source Code, and QSRSoft Website. (P. Ex. 1). The Copyright Act provides that:

[HN4] In any judicial proceedings the certificate of a registration made before or within five years after first publication of the work shall constitute *prima facie* evidence of the validity of the copyright and of the facts stated in the certificate. The evidentiary weight to be accorded the certificate of a registration made thereafter shall be within the discretion of the court.

17 U.S.C. § 410(c). Since QSRSoft has provided Certificates of Registration for the Data Engine, Source Code, and QSRSoft Website ("Website") and each of the copyright registrations is within the past five years, the registrations are entitled by statute to a *prima facie* presumption of validity. *Id.* [HN5] This presumption of validity and ownership is rebuttable. *Id.*

Although QSRSoft's registration certificates constitute *prima facie* evidence of validity, not every element of the copyrighted work is protected. Since the court must inquire as to what aspects of the work have been afforded copyright protection, [*10] it is not enough for QSRSoft to merely present the registration certificates. QSRSoft has failed to present evidence of the Data Engine and Source Code during the preliminary hearing or in its brief, but has introduced an example of the Website as Exhibit 1. Therefore, because QSRSoft has not presented sufficient evidence to support the likelihood of success on its copyright claims pertaining to the Data Engine and Source Code, we will only consider the copyright claim pertaining to the Website.

RTI argues that QSRSoft has failed "to show that it has an *original* work and not a mere compilation of unprotectable data . . . [and has] failed to satisfy its burden." (Prelim. Inj. Resp. 10)(emphasis in original). However, because proof of registration within five year after first publication of the work constitutes a *prima facie* presumption of validity, the burden does not fall upon QSRSoft to prove validity, but rather on RTI to rebut the presumption of copyright validity. 17 U.S.C. § 410(c). RTI contends that QSRSoft's copyrighted works are invalid because the Supreme Court in *Feist* has stated:

2006 U.S. Dist. LEXIS 76120, *; 84 U.S.P.Q.2D (BNA) 1297

Since facts do not owe their origin to an act [*11] of authorship, they are not original and, thus, are not copyrightable . . . copyright protection extends only to those components of the work that are original to the author, not to the facts themselves.

(Prelim. Inj. Resp. 10)(citing "*Feist*, 499 U.S. at 340" [Syllabus]). The Syllabus of *Feist*, however, does not constitute the opinion of the Supreme Court, but instead a summary of the case for the convenience of the researcher. *United States v. Detroit Lumber Co.*, 200 U.S. 321, 337, 26 S. Ct. 282, 50 L. Ed. 499 (1905). Additionally, *Feist* does not stand for the proposition that a composition of facts are beyond copyright protection or that a compilation of facts requires more than a quantum of originality required to obtain a copyright in the work. *Feist*, 499 U.S. at 361. The *Feist* Court stated:

[HN6] Facts, whether alone or as part of a compilation, are not original and therefore may not be copyrighted. A factual compilation is eligible for copyright if it features an original selection or arrangement of facts, but the copyright is limited to the particular selection or arrangement. In no event may copyright extend to the facts themselves. [*12]

Id. at 351-52. Thus, while QSRSoft cannot copyright the ISP data, QSRSoft may copyright the manner in which it displays the data. Since the Data Engine and Source Code are not before this court, we are unable to determine the validity of those works. However, as stated above, a hardcopy of the QSRSoft Website was presented at the preliminary injunction hearing. (P Ex. 7). For the Website, QSRSoft does not contend to be copyrighting the ISP data, but does claim to be copyrighting the way in which it presents the data in the graphical displays. Accordingly, we find that there is sufficient evidence that shows that QSRSoft has met its burden to show a *prima facie* presumption of validity and RTI has not presented sufficient evidence to rebut such.

2. Copying of Original Expressions

The evidence presented during the preliminary injunction hearing indicates that QSRSoft is likely to prove the direct infringement of its works by RTI. [HN7] The Copyright Act defines direct infringement as "[a]nyone who violates any of the exclusive rights of the copyright owner." 17 U.S.C. 501(a). The internet access logs demonstrate that RTI accessed the [*13] password protected copyrighted Website. The access logs also establish that

RTI employees viewed, printed, and downloaded the information while viewing the Website. By downloading and printing the Website, RTI violated QSRSoft's exclusive right to reproduce the protected works. See *Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs.*, 983 F. Supp. 1167, 1173-74 (N.D. Ill. 1997)(finding that downloading clip art constituted a violation of the plaintiff's right to reproduce its copyrighted work); *Sega Enterprises Ltd. v. Maphia*, 948 F. Supp. 923, 931-32 (N.D. Cal. 1996)(finding that the new copies of a program were created upon uploading and downloading); *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993)(finding that [HN8] uploading files containing copyrighted photographs constituted reproduction).

RTI argues that in order to prove that RTI infringed QSRSoft's copyrighted work the court must perform a "side-by-side" comparison of QSRSoft's product and RTI's product. RTI cites *Bridgmon v. Array Systems Corp.*, 325 F.3d 572 (5th Cir. 2003), to support the need for a "side-by-side" comparison. [*14] In *Bridgmon*, the Fifth Circuit affirmed the granting of summary judgment because the plaintiff failed to produce evidence that would allow the court to do a "side-by-side" comparison. However, we decline to adopt *Bridgmon*. First, the *Bridgmon* court stated that "the law of [the Fifth] [C]ircuit prohibits finding copyright infringement without a side-by-side comparison of the two works," *id.* at 577, this court is not bound by the rulings of the Fifth Circuit. Second, [HN9] the law of the Seventh Circuit, which is binding authority, does not require a "side-by-side" comparison of the products, but rather requires a substantial similarity between the plaintiff's copyrighted work and the defendant's work if there is no evidence of direct infringement. *Atari Inc.*, 672 F.2d at 614; see *Sassafras Enter. v. Roshco, Inc.*, 889 F.Supp 343 (N.D. Ill. 1995)(noting that a side-by-side comparison is not required in the Seventh Circuit). Third, since there is a substantial likelihood of direct infringement, there is no need for this court to perform a substantial similarity test in this case. Fourth, *Bridgmon* occurred at the summary judgment [*15] stage of the proceeding, after completion of discovery, rather than during the preliminary injunction stage where discovery had not been completed and where the plaintiff would have needed only to show a likelihood of success on the merits. Finally, because we are focused solely on the Website, we are able to perform the "ordinary observer" test applied in the Seventh Circuit. *Atari Inc.*, 672 F.2d at 614. Therefore, QSRSoft has a strong likelihood of showing that RTI copied original elements of the copyrighted Website.

B. Trade Secret Misappropriation

2006 U.S. Dist. LEXIS 76120, *; 84 U.S.P.Q.2D (BNA) 1297

[HN10] Under the ITSA, the court may issue an injunction if there is "actual or threatened misappropriation of a trade secret." 765 ILCS 1065/3(a). QSRSoft claims that RTI misappropriated "at least two of its trade secrets: the Specific ISP Data and the 100+ web-page displays ("Screen Shots"). (Mot. 12). [HN11] For QSRSoft to show a "better than negligible chance" on succeeding on its ITSA trade secret misappropriation claim, QSRSoft must show that (1) there is a trade secret; (2) the trade secret was misappropriated by RTI; and (3) RTI used the trade secret for business purposes. See *Composite Marine Propellers, Inc. v. Van Der Woude*, 962 F.2d 1263, 1265-66 (7th Cir. 1992) [*16] (citing 765 ILCS 1065/2).

1. Existence of Trade Secrets

[HN12] The ITSA defines a trade secret as:

[I]nformation, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that:

(1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and

(2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

765 ILCS 1065/2(d). The ITSA therefore "precludes trade secret protection for information generally known or understood within an industry even if not to the public at large," *Pope v. Alberto-Culver Co.*, 296 Ill. App. 3d 512, 694 N.E.2d 615, 617, 230 Ill. Dec. 646 (Ill. App. Ct. 1998), and "requires a plaintiff to take 'affirmative measures' to prevent others from using [the] information." *Jackson v. Hammer*, 274 Ill. App. 3d 59, 653 N.E.2d 809, 816, 210 Ill. Dec. 614 (Ill. App. Ct. 1995); see *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 722 (7th Cir. 2003) [*17] (noting that the ITSA "prevents a plaintiff who takes no affirmative measures to

prevent others from using its proprietary information from obtaining trade secret protection"). [HN13] In determining whether a trade secret exists, Illinois courts generally look to: (1) the extent that the information is known outside of the business; (2) the extent that the information is known to employees and others within the business; (3) the measures taken to protect the information from outsiders; (4) the value of the information to competitors; (5) the amount of time, money, and effort to develop the information; and (6) the ease that the information could be acquired by others. *Learning Curve Toys*, 342 F.3d at 722. We disagree with RTI's contention that QSRSoft does not have any trade secret rights in the Specific ISP Data and Screen Shots.

The evidence shows that QSRSoft is likely to succeed in establishing the existence of valid trade secrets. First, although the ISP data is not stored on QSRSoft computers and the ISP data is owned by McDonald's franchisees, how QSRSoft compiles and manipulates the Specific ISP Data for use in the DotComm System is not known to competitors in the [*18] industry. Second, QSRSoft has taken reasonable measures to protect its trade secrets from the general public and competitors through the use of licensing agreements, a password protected website, and generally keeping its trade secrets out of the public display at conventions. See *Stampede Tool Warehouse, Inc. v. May*, 272 Ill. App. 3d 580, 651 N.E.2d 209, 216, 209 Ill. Dec. 281 (Ill. App. Ct. 1995) (finding that trade secret had not been waived when reasonable efforts were taken to protect secrecy of trade secrets from competitors). Third, QSRSoft has presented evidence that show it invested "over two and a half years, more than \$ 2,000,000, and employed three full-time software developers and system architects" to develop the DotComm System. (Mot. 13). Finally, due to the amount of data contained in the ISP, approximately 315 tables consisting of approximately one million pieces of information, and the fact that the Specific ISP Data represents approximately one percent of the data in the ISP, competitors would have to spend a large amount of time and effort, just as QSRSoft has done, in order to ascertain the precise data needed to determine the Specific ISP Data.

RTI contends that QSRSoft does not have [*19] valid trade secrets in the ISP Data or Screen Shots, noting that QSRSoft "spends only two of fifteen pages in its Motion discussing its alleged trade secret claim" (Prelim. Inj. Resp. 10). RTI argues that QSRSoft cannot show the validity of the QSRSoft trade secrets because QSRSoft never introduced either the Specific ISP Data or Screen Shots into evidence. RTI further states that QSRSoft "failed to put into evidence exactly what information [QSRSoft] is referring to when it refers to its Specific ISP Data and DotComm Screen Shots as trade secrets." (Prelim. Inj. Resp. 11). In support of its argu-

2006 U.S. Dist. LEXIS 76120, *; 84 U.S.P.Q.2D (BNA) 1297

ment, RTI contends that the Seventh Circuit in *Composite Marine Propellers, Inc.*, stated that "[i]t is not enough to point to broad areas of technology and assert that something there must have been a secret and misappropriated" and that "[t]he plaintiff must show concrete secrets." (Prelim. Inj. Resp. 11)(emphasis in brief)(quoting 962 F.2d at 1265). In *Composite Marine Propellers*, however, the judge submitted the trade secret issues to the jury, rather than rule at the preliminary injunction stage. *Id.* at 1266. Additionally, RTI's [*20] brief and exhibits support the notion that QSRSoft did in fact show concrete trade secrets. First, RTI notes that "the DotComm product . . . manipulates data that belongs to third[-]parties." (Prelim. Inj. Resp. 2). This "manipulated data" is the Specific ISP Data trade secret referred to by QSRSoft. See, e.g., *ISC-Bunker Ramo Corp. v. Altech, Inc.*, 765 F.Supp. 1310 (N.D. Ill. 1990)(finding technical manual compilations of information and procedures that were useful to financial institutions to be trade secrets under the ITSA). Second, the declaration of Barbra Morrison, (D. Ex. B), notes that she observed QSRSoft's "demonstration of its DotComm System on the big screen television" at the McDonald's Convention in May 2006. (D. Ex. B at 3). One cannot find a better way of pointing out concrete examples of the Screen Shots than on a big screen television. If at the trial stage QSRSoft is "vague about the nature of [its trade] secrets," then RTI's argument would be valid under Seventh Circuit precedent. (Prelim. Inj. Resp. 11)(quoting *Composite Marine Propellers, Inc.*, 962 F.2d at 1266). However, at this stage of the proceedings, QSRSoft must only [*21] show that it has a better than negligible chance" of succeeding on the merits of its trade secret misappropriation claim, which includes showing the existence of trade secrets. *Washington*, 181 F.3d at 845.

RTI alternatively argues that QSRSoft did not reasonably maintain the secrecy of QSRSoft's trade secrets and QSRSoft thereby waived the trade secrets. RTI contends that in *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002, 104 S. Ct. 2862, 81 L. Ed. 2d 815 (1984), "the United States Supreme Court has stated expressly that trade secrets are *extinguished*" when provided to a third-party that is not obligated to protect the confidentiality of the trade secrets." (Prelim. Inj. Resp. 11)(emphasis in original). RTI contends that the Supreme Court has stated:

Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others. Information that is public knowledge or that is generally known in an industry cannot be a trade secret. *If an individual discloses*

*his trade secret to others who are under no obligation to protect the confidentiality of the [*22] information, or otherwise publicly discloses the secret, his property right is extinguished.*

(Prelim. Inj. Resp. 11)(citing *Ruckelshaus*, 467 U.S. at 1002)(emphasis in brief). However, in *Ruckelshaus*, the Supreme Court was faced with the question of whether the *Takings Clause of the Fifth Amendment* applied to the Environmental Protection Agency's ("EPA") public disclosure of a trade secret, an intangible property, in the same way it would to tangible property. 467 U.S. at 1001-02. The particular phrase cited by RTI was used by the Supreme Court to compare trade secrets to tangible property in finding that the plaintiff, Monsanto, had a property right that is protected by the *Takings Clause* since trade secrets have many of the characteristics of tangible property. *Id.* at 1001-04. Thus, the statement referred to by RTI is not a "clear" statement that any disclosure to a third-party waives a trade secret, but rather is a general statement of the law. (Prelim. Inj. Resp. 11).

RTI similarly cites *Skoog v. McCray Refrigerator Co.*, 211 F.2d 254, 257 (7th Cir. 1954), stating that "[t]he Seventh Circuit has similarly [*23] found that the disclosure of a trade secret to those under no obligation to protect its confidentiality destroys the trade secret." (Prelim. Inj. Resp. 11). However, *Skoog* is distinguishable from the instant action. In *Skoog*, the court found that the defendant could not misappropriate the trade secret at issue, a refrigerated cabinet, because the trade secret was no longer hidden from the public. 211 F.2d at 257-58. Specifically, the trade secret was extinguished because the plaintiff's refrigerated cabinet had been in unrestricted use in the plaintiff's grocery store, visible to anyone that entered the store, and the defendant had expressly stated that it did not accept the plaintiff's non-disclosure agreement. *Id.* In the instant action, the evidence establishes that QSRSoft's trade secrets were sufficiently guarded from the public. The efforts taken by QSRSoft to hide its trade secret from competitors such as RTI include: guarding the DotComm System with licensing agreements and a password protected website; not showing the Specific ISP Data or Data Engine to potential customers and competitors at conventions; typically only showing prospective customers [*24] and competitors less than five percent of the DotComm System at conventions; typically only showing prospective customers and competitors less than five percent of the Screen Shots at conventions; not showing the DotComm web interface during demonstrations; and not allowing customers and competitors to view the DotComm source code. These efforts are more than reasonable to establish a better than negligible chance that QSRSoft will be able

2006 U.S. Dist. LEXIS 76120, *; 84 U.S.P.Q.2D (BNA) 1297

to show that it did not waive its trade secrets. *See, e.g., Web Communications Group, Inc. v. Gateway 2000, Inc.*, 889 F. Supp. 316, 320 (N.D. Ill. 1995) (holding that the plaintiff's trade secret misappropriation claim failed "because [plaintiff] took virtually no steps to protect the confidentiality" of the trade secret) (noting that none of the documents relating to the trade secret were marked as confidential (as was the plaintiff's policy with trade secrets), there was not a confidentiality agreement with the defendant, the plaintiff disclosed "either dummies or specifications" for the trade secret at issue to suppliers and competitors, and the plaintiff's president acknowledged that the competitor would be able to use the disclosed [*25] information for its own benefit); *Stampede Tool Warehouse*, 651 N.E.2d at 216 (finding that [HN14] trade secret had not been waived when reasonable efforts were taken to protect secrecy of trade secrets from competitors); *cf. Skoog*, 211 F.2d at 257 (stating that it is "well established that there can be no confidential disclosure where there has been a prior disclosure to the public without reservation") (emphasis added).

RTI also argues that because an authorized user accessed the DotComm System and since QSRSoft did not immediately discontinue access to the DotComm System for that user, that QSRSoft has placed its trade secrets into the public domain. However, the evidence supports the finding that the only reported breach of QSRSoft's efforts to keep its trade secrets hidden was performed and traced back to RTI employees, Clutter and Starkey, who viewed, downloaded, and printed information while on the password protected website. *See* (P. Ex. 7, 8, 9, 10, 11) (showing internet access logs of alleged unauthorized users). Additionally, the fact that RTI understood that the DotComm System could only be accessed with the correct login information supports [*26] the claim that RTI was aware that QSRSoft had taken measures to protect its trade secrets. (D. Ex. D) (showing email from Matejka to Sten with DotComm access information). RTI's surreptitious access to the password protected website does not negate the fact that QSRSoft took reasonable efforts to protect its trade secrets. *Learning Curve Toys*, 342 F.3d at 725. Therefore, based on the evidence, we find that there is a strong likelihood that QSRSoft's claimed trade secrets are protected by the ITSA.

2. Trade Secret Misappropriation & Use of the Trade Secrets

The evidence also shows that QSRSoft has a strong likelihood of showing that RTI misappropriated QSRSoft's trade secrets. The ITSA defines misappropriation as:

[HN15] (1) acquisition of a trade secret of a person by another person who knows or has reason to know that the trade secret

was acquired by improper means; or (2) disclosure or use of a trade secret of a person without express or implied consent by another person who:

(A) used improper means to acquire knowledge of the trade secret; or

(B) at the time of disclosure or use, knew or had reason to know that knowledge of the trade secret was:

(I) [*27] derived from or through a person who utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

765 ILCS 1065/2(b).

The internet access logs establish that RTI employees repeatedly accessed the DotComm System through the password protected website, viewed and printed the Screen Shots, and downloaded and saved the DotComm data archive containing historical FAF data that establishes the Specific ISP Data. Due to the amount of time and money expended by QSRSoft software developers and system architects to compile, manipulate, and solve the data contained in the ISP, coupled with the fact that there was no other product on the market that analyzed the data in such a way, at the very least, the information downloaded and saved by RTI served as a guide to RTI. Such a [*28] guide would have made it easier for RTI to develop Reports+, a direct competitor to the DotComm System. Even if RTI did not directly copy QSRSoft's

trade secrets, using the trade secrets as a guide likely rises to the level of misappropriation. See *Affiliated Hosp. Prods., Inc. v. Baldwin*, 57 Ill. App. 3d 800, 373 N.E.2d 1000, 1006, 15 Ill. Dec. 528 (Ill. App. Ct. 1978)(stating that "even accepting their denial of any literal copying of [the] drawings, these drawings aided defendants in the design [of the infringing machinery], if only to demonstrate what pitfalls to avoid").

Additionally, RTI's competing product, Reports+, bears a strong resemblance to QSRSoft's DotComm System. First, both products use identical information, the Specific ISP Data contained within the ISP, to create reports for McDonald's franchisees. Second, the look and feel of the graphical summaries on the DotComm System's main page, (P Ex. 6), is nearly identical to RTI's brochure advertising Reports+. (P Ex. 7). Third, the information listed on the DotComm System's main page is strikingly similar to RTI's brochure advertising Reports+. Fourth, Matejka, who has used both products, testified that Reports+ "looked very similar to [*29] the QSRSoft Product." (R. 47). These similarities exist despite the fact that RTI claims that "[t]he RTI Development Team did not download, use, or otherwise refer to [the] 'QSRSoft Data Engine,' including the source code associated with that engine ... in its development of the RTI Product." (D. Ex. A). RTI argues that "[t]he marketing brochure literally has nothing to do with the programming code for the RTI product." (Prelim. Inj. Resp. 10). However, we do not find it plausible that RTI would distribute sales brochures that aim at attracting potential customers for a feature of the product that does not exist.

RTI argues that it could not misappropriate QSRSoft's trade secrets because RTI did not acquire the trade secrets through "improper means." (Prelim. Inj. Resp. 1). [HN16] The ITSA defines "improper means" to include "theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means." 765 ILCS 1065/2(a). Evidence shows that RTI acquired access to the DotComm System password protected website by inducing FAF, through Matejka, [*30] to breach its confidential relationship with QSRSoft, as contained in the Agreement. According to Matejka, although he did not read the Agreement, he understood the Agreement to prohibit FAF from distributing the password to anyone outside the FAF organization. (R. 44). FAF was bound by the Agreement once Matejka accessed the password protected website with the understanding that the password was not to be distributed to others outside of FAF. See *Wood v. Wabash County*, 309 Ill. App. 3d 725, 722 N.E.2d 1176, 1179, 243 Ill. Dec. 107 (Ill. App. Ct. 1999)(stating that [HN17] an implied-in-fact contract is one in which an agreement may be inferred by perform-

ance of the parties). Thus, a confidential relationship existed between QSRSoft and FAF, and the evidence shows that RTI induced FAF to breach the confidential relationship.

RTI also contends that "[t]here is absolutely no evidence that RTI knew that FAF was not authorized" to send RTI access information for the DotComm System. (Prelim. Inj. Resp. 11). However, this argument belies that RTI received the information from a FAF representative, rather than going directly to QSRSoft. In an email from Sten to Matejka, Sten requested specific information regarding the [*31] DotComm System, including sample reports, cost, internet speed, and timing. RTI could only acquire this information through a password protected website, which RTI could not access unless it signed a licensing agreement or received the information from FAF. Additionally, as stated above, RTI employees downloaded and saved the DotComm data archive containing historical FAF data that establishes the Specific ISP Data. RTI cannot claim that it did not know or understand that FAF was not authorized to send RTI access information for the password protected website of a potential competitor.

Finally, RTI argues that "the very terms of [QSRSoft's] own License Agreement allow FAF to do exactly what it did in this case—disclose DotComm Products to a third-party (such as RTI)." We disagree. The Agreement states that:

... Licensee may *not* use the DotComm Product in a production environment, to produce revenue for Licensee, to demonstrate or provide Dotcomm Product to any other party or to develop software owned by any party other than QSRSoft.

(P. Ex. 3)(emphasis added). Although the licensing agreement may contemplate a breach of the Agreement, such a contemplation cannot [*32] be interpreted to mean that FAF could disclose the DotComm System to RTI. Therefore, the similarities between the DotComm System, combined with the unfettered access by RTI's employees to the DotComm System, as well as QSRSoft's alleged investment of "over two and a half years [and] more than \$ 2,000,000 ...," (Mot. 13), and RTI's relative lack of knowledge in this type of reporting system, as evidenced by RTI's need to access the DotComm System password protected website, give strong support to QSRSoft's claims of trade secret misappropriation and use of the trade secrets for business purposes by RTI.

II. Inadequate Remedy at Law & Irreparable Harm

2006 U.S. Dist. LEXIS 76120, *; 84 U.S.P.Q.2D (BNA) 1297

[HN18] There is a rebuttable presumption of irreparable harm to a plaintiff in cases of trade secret misappropriation and copyright infringement. *Atari Inc.*, 672 F.2d at 620; *ISC-Bunker Ramo Corp.*, 765 F.Supp. at 1329. A defendant can rebut this presumption by demonstrating that the plaintiff will not suffer any harm if the injunction is not granted. See *Wainwright Secs., Inc. v. Wall Street Transcript Corp.*, 558 F.2d 91, 94 (2d Cir. 1977)(explaining the rebuttable presumption). QSRSoft [*33] alleges that it has expended "over two and a half years, more than \$ 2,000,000, and employed three full-time software developers and system architects" to develop the DotComm System. (Mot. 13). QSRSoft claims that up until the point when QSRSoft introduced the DotComm System, there had not been a product on the market that similarly isolated and compiled the amount and type of data like the DotComm System. While RTI also has access to the ISP data and advertises to franchisees, RTI's expertise lies in accounting software which uses limited amounts of the ISP data. Even if QSRSoft were to succeed on its claims of copyright infringement and trade secret misappropriation, assessing the monetary value of QSRSoft's head start in the market would be nearly impossible. If RTI is allowed to market Reports+ to consumers, QSRSoft's head start will be lost and QSRSoft will be unable to reap the benefits as the initial market entrant, which would make assessing damages difficult. See *Ty*, 237 F.3d at 903 (stating that [HN19] "it is virtually impossible to ascertain the precise economic consequences of intangible harms, such as damage to reputation and loss of goodwill"); *Reinders Bros., Inc. v. Rain Bird E. Sales Corp.*, 627 F.2d 44, 53 (7th Cir. 1980) [*34] (noting that damage to servicing clients efficiently constitutes irreparable harm). Additionally, RTI has failed to demonstrate that QSRSoft will not suffer any harm if the injunction is not granted and failed to note any harm that would come to RTI if the injunction is granted. Instead, RTI simply states that QSRSoft "offered absolutely no evidence of its alleged

irreparable harm at the Evidentiary Hearing." (Prelim. Inj. Resp. 15). Thus, we find that the balance of harms is clearly in favor of QSRSoft. Evidence establishes that QSRSoft is likely to prove material infringement in its copyright and trade secret misappropriation claims and the harm to RTI's potential sales of Reports+ is offset by the irreparable harm it may cause QSRSoft's business, reputation, and customer goodwill. QSRSoft also has shown no adequate remedy at law exists.

IV. Public Interest

We find that granting an injunction is also in the public interest. [HN20] The public is generally interested in upholding intellectual property rights, encouraging innovation and creativity, and rewarding those that take the risk and invest resources in pursuit of such innovation and creativity. See generally, *United States Constitution*, Art. I, sec. 8, cl. 8 [*35]. Additionally, the public is unlikely to suffer any harm if RTI refrains from accessing, downloading, or copying the DotComm System. The public will also not suffer any harm if RTI is not allowed to destroy any materials that may be necessary to the instant matter, or if RTI is required to return the material that RTI acquired while accessing the DotComm System. Finally, since RTI has indicated that it "has no plan to offer the RTI Reports+ product during the pendency of this litigation" the public is unlikely to be harmed since Reports+ would not be on the market for sale. (D. Ex. B).

CONCLUSION

Based on the foregoing analysis, we grant QSRSoft's motion for a preliminary injunction.

Samuel Der-Yeghiayan

United States District Court Judge

Dated: October 19, 2006

C

LEXSEE 1998 U.S. DIST. LEXIS 3188

I

Cited

As of: Jan 25, 2008

MERRILL LYNCH, PIERCE, FENNER & SMITH, INC., Plaintiff, v. GEORGE H. CROSS, III, Defendant.

98 C 1435

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

1998 U.S. Dist. LEXIS 3188

March 12, 1998, Decided

DISPOSITION: [*1] Merrill Lynch's renewed motion for a temporary restraining order granted.

quo until the arbitration panel decided the case on the merits.

CASE SUMMARY:

OUTCOME: The court granted the investment firm's motion for a temporary restraining order.

PROCEDURAL POSTURE: Plaintiff investment firm filed an action against defendant employee alleging violations of an employment agreement and of the Illinois Trade Secrets Act, 765 Ill. Comp. Stat. 1065/1 et seq. The investment firm filed a motion for a temporary restraining order pending an arbitration hearing.

LexisNexis(R) Headnotes

OVERVIEW: The employee signed an employment agreement with the investment firm, and the agreement included a provision prohibiting the employee from soliciting clients of the investment firm for a period of one year after leaving employment there. He later left the investment firm and began working for one of its competitors. He wrote letters to his former clients so that they would know how to reach him and included paperwork for them to sign if they wanted to transfer their accounts to his new firm. The investment firm claimed that this conduct constituted solicitation, and the parties agreed to submit the matter to arbitration. The court held that the investment firm was entitled to a temporary restraining order pending arbitration. The court ruled that (1) the investment firm showed a better than negligible chance of prevailing on the merits; (2) the affidavits submitted by the investment firm supported its assertions of irreparable harm, an inadequate remedy at law, and that the balance of hardships was in its favor; and (3) issuing a temporary restraining order would preserve the status

Civil Procedure > Remedies > Injunctions > Preliminary & Temporary Injunctions
Civil Procedure > Remedies > Injunctions > Temporary Restraining Orders

[HN1] A party seeking a temporary restraining order has the burden of establishing each of the following: a better than negligible chance of prevailing on the merits; the absence of an adequate remedy at law; and irreparable harm if the temporary restraining order is not granted. Once the movant establishes these three elements, the court must balance the harm to the movant if the injunction is not issued with the harm to the defendant if it is issued improvidently. The equitable purpose of a temporary restraining order is to minimize hardship to the parties pending the ultimate resolution of the lawsuit.

Labor & Employment Law > Employment Relationships > Employment Contracts > Conditions & Terms > Trade Secrets & Unfair Competition > Former Employer's Customers

[HN2] There is a significant distinction between mere contact and solicitation. The direct solicitation of cus-

1998 U.S. Dist. LEXIS 3188, *

tomers, as opposed to general advertisement, suggests a private communication directed at a person known by the solicitor to have an immediate or potential need for insurance.

Labor & Employment Law > Employment Relationships > Employment Contracts > Conditions & Terms > Trade Secrets & Unfair Competition > Trade Secrets Law > Protected Information > Customer Lists

[HN3] Customer lists are entitled to trade secret protection under Illinois law.

Civil Procedure > Alternative Dispute Resolution > Arbitrations > General Overview

Civil Procedure > Remedies > Injunctions > Preliminary & Temporary Injunctions

[HN4] District courts are not precluded from issuing preliminary injunctive relief pending arbitration. Pro-arbitration policies are furthered by permitting a district court to preserve the meaningfulness of the arbitration by granting injunctive relief.

COUNSEL: For MERRILL LYNCH PIERCE FENNER & SMITH INC, plaintiff: John H. Anderson, Jerome F. Buch, Seyfarth, Shaw, Fairweather & Geraldson, Chicago, IL.

For GEORGE H CROSS, III, defendant: Lawrence Andrew Brehm, Jeffrey Ray Rosenberg, Schuyler, Roche & Zwirner, P.C., Chicago, IL.

JUDGES: Charles P. Kocoras, United States District Judge.

OPINION BY: Charles P. Kocoras

OPINION

MEMORANDUM OPINION AND ORDER

CHARLES P. KOCORAS, District Judge:

This matter is before the court on the plaintiff's renewed motion for a temporary restraining order pending an arbitration hearing on the merits of the plaintiff's case against the defendant. For the foregoing reasons, the court grants the plaintiff's motion.

DISCUSSION

Plaintiff Merrill Lynch, Pierce, Fenner & Smith Inc. ("Merrill Lynch"), filed suit against George H. Cross, III, for alleged violations of the express provisions of his employment agreement with Merrill Lynch, for viola-

tions of the Illinois Trade Secrets Act, 765 ILCS 1065/1 *et seq.*, for breach of the duty of loyalty, and unfair competition. Merrill Lynch claims that Cross solicited Merrill Lynch [*2] clients and retained confidential client information and other trade secrets after he resigned from Merrill Lynch on March 9, 1998. Merrill Lynch seeks a temporary restraining order ("TRO") to prevent Cross from soliciting clients that he serviced while employed at Merrill Lynch. The parties agreed to submit their dispute to arbitration and intend to have the merits of this case resolved at an arbitration hearing before a panel of arbitrators in accordance with Rule 12335(g) of the National Association of Securities Dealers Code of Arbitration Procedure.

Merrill Lynch claims that Cross violated the express provisions of his employment agreement. Specifically, the agreement provides:

In the event of termination of my services with Merrill Lynch for any reason, I will not solicit for a period of one year from the date of termination of my employment in any community or city served by the office of Merrill Lynch, ... at which I was employed at any time, any of the clients of Merrill Lynch whom I served or whose names became known to me while in the employ of Merrill Lynch.

[HN1] A party seeking a TRO has the burden of establishing each of the following: (1) a better than negligible [*3] chance of prevailing on the merits; (2) the absence of an adequate remedy at law; and (3) irreparable harm if the TRO is not granted. *Artipresent GmbH Vertrieb Internationaler Collectionen für den Wohnbereich v. Emruss Corp.*, 1997 U.S. Dist. LEXIS 12923, No. 97 C 5130, 1997 WL 534358 (N.D. Ill. 1997). Once the movant establishes these three elements, the court must balance the harm to the movant if the injunction is not issued with the harm to the defendant if it is issued improvidently. *Id.* Similar to a preliminary injunction, the equitable purpose of a TRO is to minimize hardship to the parties pending the ultimate resolution of the lawsuit. *Faheem-El v. Klinkar*, 841 F.2d 712, 717 (7th Cir. 1988).

In this case, Merrill Lynch has provided the court with strong reasons for granting a TRO. First, Merrill Lynch has provided evidence, by way of affidavits, showing that Cross has contacted Merrill Lynch customers that he served while employed at Merrill Lynch. Merrill Lynch contends that the purpose of Cross' contact with Merrill Lynch customers is to induce them to move their accounts to his new employer, Dain Rauscher, in

1998 U.S. Dist. LEXIS 3188, *

violation of Cross' employment agreement with Merrill Lynch. Cross admits that [*4] he has contacted Merrill Lynch clients, but disputes that such contact was in fact solicitation. Cross claims that he merely advised these customers that he had resigned from Merrill Lynch in order to work for Dain Rauscher in Chicago.

[HN2] Although there is a significant distinction between mere contact and solicitation, courts have found conduct similar to Cross' conduct in this case to be solicitation. In *Tomei v. Tomei*, 235 Ill. App. 3d 166, 602 N.E.2d 23, 26, 176 Ill. Dec. 716 (Ill. App. Ct. 1992), the court explained: "The direct solicitation of ... customers, as opposed to general advertisement, suggests a private communication directed at a person ... known by the solicitor to have an immediate or potential need for insurance." In this case, Cross personally contacted Merrill Lynch customers and admits that these customers have a need for his financial services. Moreover, Cross did not simply contact previous customers to provide them with information as to his whereabouts. In one affidavit the affiant states that Cross sent a letter to a Merrill Lynch customer, enclosing a form for the customer to complete to transfer his account to Dain Rauscher. Thus, it appears that Cross [*5] is engaging in conduct that clearly constitutes solicitation. Further, we find significant that Cross personally phoned the Merrill Lynch customers, using confidential records and information he obtained from Merrill Lynch. [HN3] Customer lists are entitled to trade secret protection under Illinois law. See *IDS Financial Services, Inc. v. Smithson*, 843 F. Supp. 415, 418 (N.D. Ill. 1994). Based on the foregoing, the court finds that Merrill Lynch has shown a better than negligible chance of prevailing on the merits of their claims.

The affidavits provided by Merrill Lynch also support their assertion of irreparable harm, an inadequate remedy at law, and that the balance of hardships is in their favor. The affiants state that Cross has contacted Merrill Lynch customers, has used confidential customer information to do so, and has used Merrill Lynch's computer system to generate financial records. As stated previously, one affiant states that Cross sent a form to a Merrill Lynch customer which would transfer the customer's account to Dain Rauscher if completed. Merrill Lynch will suffer irreparable harm from the disclosure of trade secrets, customer lists, and other information because [*6] Merrill Lynch may lose clients and suffer loss to its goodwill and business reputation from Cross' actions. See e.g., *Merrill Lynch, Pierce, Fenner & Smith v. Bradley*, 756 F.2d 1048, 1055 (4th Cir. 1985) (Merrill Lynch faced "irreparable non-compensable harm in the loss of its customers"). If clients discover that Merrill Lynch has somehow permitted their "confidential" information to be disclosed to Dain Rauscher, they may lose trust and confidence in Merrill Lynch. See e.g., *Merrill*

Lynch, Pierce, Fenner & Smith v. Kramer, 816 F. Supp. 1242, 1247 (N.D. Ohio 1992) ("irreparable and immeasurable harm lies in the fact that Merrill Lynch clients when they discover that their financial information ... have been disclosed, will lose trust and confidence in Merrill Lynch.") The balance of hardships, in this case, also favors the plaintiff. The harm to Merrill Lynch from the defendant's use and disclosure of confidential, customer information and trade secrets clearly outweighs any harm to Cross from refraining, for a very limited period of time, from contacting such customers and using Merrill Lynch's trade secrets and customer information.

In a similar case involving Merrill Lynch, [*7] the Seventh Circuit found that the district court did not abuse its discretion in granting a TRO enjoining the defendants, two account executives for Merrill Lynch, from disclosing Merrill Lynch records and soliciting clients of Merrill Lynch. See *Merrill Lynch, Pierce, Fenner & Smith v. Salvano*, 999 F.2d 211, 215 (7th Cir. 1993). The Seventh Circuit found that evidence indicating that the defendants took documents and information regarding Merrill Lynch customers and used that information to solicit customers was sufficient to support the district court's determination that irreparable harm would result to Merrill Lynch. *Id.* This evidence also supported the district court's determination that there was an inadequate remedy at law. *Id.* Although the defendants would suffer some harm during the pendency of the TRO, the Seventh Circuit stated that the district court was right in finding that the denial of the TRO would inflict greater injury on Merrill Lynch. *Id.* Significantly, the Seventh Circuit noted that "the TRO served to maintain the status quo without prejudice to the merits of any of the parties' claims or defenses until an arbitration panel could consider the [*8] issues presented."

Likewise, in this case, a TRO would preserve the status quo without prejudice to either party until an arbitration panel considers the merits of Merrill Lynch's case. We note that the Seventh Circuit said in *Salvano* that [HN4] "district courts are not precluded from issuing preliminary injunctive relief pending arbitration." *Salvano*, 999 F.2d at 214. To the contrary, the pro-arbitration policies increasingly reflected in cases "are furthered ... by permitting a district court to preserve the meaningfulness of the arbitration" by granting injunctive relief." *Id.* Accordingly, the court grants Merrill Lynch's motion for a temporary restraining order.

IT IS HEREBY ORDERED AND DECREED: A temporary restraining order shall issue immediately and stay in effect until March 22, 1998.

1. The defendant is restrained, directly or indirectly, whether alone or in concert with others, from:

1998 U.S. Dist. LEXIS 3188, *

(a) contacting any client of Merrill Lynch whom defendant served or whose name became known to defendant while in the employ of Merrill Lynch;

(b) accepting any business or account transfers from any customers of Merrill Lynch whom defendant, or anyone acting on defendant's behalf, [*9] has already contacted for the purpose of doing business with defendant's present employer; and

(c) using, disclosing, or transmitting for any purpose, the information contained in the records of Merrill Lynch, including, but not limited to, the names, addresses, and financial information of said clients.

2. Pending a preliminary injunction hearing before this court, and pursuant to the requirements of *sections 3 and 4* of the Federal Arbitration Act, 9 U.S.C. §§ 3-4, the parties are directed to proceed toward an expedited arbitration hearing on the merits before a duly appointed panel of arbitrators in accordance with Rule 10335(g) of the National Association of Securities Dealers Code of Arbitration Procedure.

CONCLUSION

For the reasons set forth above, the court grants Merrill Lynch's renewed motion for a temporary restraining order.

Charles P. Kocoras

United States District Judge

Dated: March 12, 1998

D

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION**

**C.H. ROBINSON WORLDWIDE, INC., a
Delaware Corporation,**

Plaintiff,

V.

JEFFREY R. SIEKMANN, an individual,

Defendant.

Case No.: _____

**[PROPOSED] TEMPORARY
RESTRAINING ORDER**

ORDER

This cause coming to be heard on Plaintiff's, C.H. Robinson Worldwide, Inc. ("C.H. Robinson"), Emergency Motion for Temporary Restraining Order and Preliminary Injunctive Relief, and Motion for Limited Expedited Discovery and to Preserve Evidence, this Court having reviewed and considered C.H. Robinson's Verified Complaint for Injunctive and Other Relief and the accompanying Declarations filed therewith, and having heard the arguments of counsel, the Court hereby finds and concludes as follows:

1. This is a civil action for violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* and the Illinois Trade Secrets Act, 765 ILCS § 1065 *et seq.*, and for breach of contract and conversion;
2. This Court has personal jurisdiction over the parties and venue is proper in this Court;
3. The Court determines that C.H. Robinson has satisfied all the requirements for the issuance of a temporary restraining order, and

IT IS HEREBY ORDERED AS FOLLOWS:

- (I) That Siekmann, his officers, agents, servants, employees, attorneys and all parties in active concert or participation with him, are enjoined from using or disclosing any confidential or proprietary information that Siekmann obtained from C.H. Robinson;
- (II) That Siekmann, his officers, agents, servants, employees, attorneys and all parties in active concert or participation with him, are enjoined and ordered to account for and return to C.H. Robinson all originals and all copies of files, data, and information removed from C.H. Robinson, including, but not limited to, the confidential and proprietary customer information, that Siekmann obtained from C.H. Robinson;
- (III) That Siekmann, his officers, agents, servants, employees, attorneys and all parties in active concert or participation with him, are hereby ordered to preserve all discs and electronic storage devices in their custody, possession and control to which Siekmann had access, and to turn over to a third-party investigator representative of C.H. Robinson all electronic storage media in their custody, possession or control, including, but not limited to, discs and hard drives accessible to Siekmann on which C.H. Robinson's information may reside and that C.H. Robinson be permitted to image and analyze said media and devices to recover and account for C.H. Robinson's confidential information.
- (IV) That Siekmann is ordered to provide access for inspection to the outside email account jsiek@cox.net to which he emailed C.H. Robinson information from his

C.H. Robinson email account and any other e-mail account in his custody or control;

- (V) That Siekmann is enjoined from contacting or conducting business with any C.H. Robinson customer whose information he improperly accessed and/or misappropriated;
- (VI) That Siekmann is enjoined from contacting or conducting business with any C.H. Robinson customer with whom he conducted business on behalf of C.H. Robinson within the twenty-four (24) months preceding issuance of this Order;
- (VII) The matter is set for preliminary injunction hearing on _____, 2008 at _____ .m.
- (VIII) This Order shall remain in full force and effect until _____, 2008 unless extended by the Court or by agreement of the parties, except that either party may move to modify the Order with proper notice.
- (IX) No bond shall be required for issuance of this Order.

IT IS SO ORDERED:

DATED this ____ day of _____, 2008.

UNITED STATES DISTRICT JUDGE